LAB³

Cloud Adoption Guide

A cloud practitioner's guide to achieve more with Microsoft Azure's NZ North region

Microsoft Solutions Partner

CONTENTS

Accelerating New Zealand's Digital Future

by Vanessa Sorenson
Chief Partner Officer ANZ, Microsoft

It is an exciting time for Microsoft as we build the Azure NZ North Datacentre region. This new, local Azure region represents more than just infrastructure and services – it's an opportunity to super-charge New Zealand's digital transformation. NZ North will create a sustainable, local home for New Zealand's data at a scale and speed beyond anything we've seen before.

With the North region now launching, the challenge for New Zealand businesses is to understand how they can securely and confidently accelerate cloud adoption and access the power, resilience, and efficiencies of Azure's local cloud infrastructure.

The LAB[3] Cloud Adoption Guide is a great tool to help business leaders and IT decision makers answer many of the questions they might be grappling with, and gain clarity on the opportunities this new Azure region introduces. I highly recommend it as an informative guide on the critical considerations and decisions required during your organisation's cloud journey.

With their strong customer-centric approach, LAB[3] is a valued Microsoft partner that has leveraged their expert Azure knowledge and innovative accelerators to achieve impressive outcomes for their New Zealand clients. Together Microsoft and LAB[3] have partnered to guide many customers with complex legacy environments and challenging requirements to unlock the full benefits of their cloud investment.

Like us, LAB[3] shares the goal of delivering practical, impactful solutions, for customers; whether migration services, building foundations and Landing Zones, or aligning AI technologies with real business requirements and outcomes. LAB[3] keeps customers at the heart of everything they do.

Warm regards
Vanessa Sorenson

INTRODUCTION

Achieving more with Azure NZ North

by Lachlan White | Chief Technology Officer, LAB³

With the launch of the New Zealand North region for Microsoft Azure imminently approaching, Business Leaders and IT Leaders in New Zealand find themselves at a pivotal moment.

As the region opens its doors it presents a wealth of opportunities for organisations to accelerate and enhance their digital transformation efforts. Our goal is to empower organisations to make informed decisions that drive business value, reduce risk, minimise regrettable spending, and increase speed whilst optimising cost and ensuring compliance with regulatory standards.

LAB³ has designed this playbook to provide practical and actionable insights for C-suite and technology leaders based on our extensive local and international experience in Australia and New Zealand to accelerate cloud adoption.

Cloud adoption is much more than a new infrastructure platform(s); it is a strategic business move that can significantly enhance operational efficiency, agility, and innovation. Organisations can leverage Microsoft Azure to reduce dependency on legacy infrastructure, scale resources dynamically based on demand, and leverage emerging technologies such as AI and Machine Learning to gain a competitive advantage. However, the journey to the cloud is complex and requires strategic planning and an understanding of your organisation's current state and future goals.

At LAB³, we understand that every organisation's cloud journey is different, but not holistically unique. Therefore, this playbook is not a one-size-fits-all solution, but a comprehensive guide tailored to the diverse needs and challenges faced by leaders in New Zealand.

This playbook covers the critical aspects of cloud adoption. The initial activities such as assessing the cloud readiness of your organisation and rationalising your digital estate will help you develop the business justification to implement wider changes. Later chapters provide guidance on enhancing value in Azure by establishing a robust cloud foundation and implementing hybrid cloud strategies.

Remember that cloud adoption is a continuous process of learning and improvement. By leveraging the insights and strategies outlined in this playbook, you can leapfrog others who may get stuck in the complexities of cloud adoption.

Enable your organisation to reap the maximum benefits from Microsoft Azure's NZ North Region. Together let's pave the way for a future where technology drives innovation, efficiency and growth.

Lachlan White
Chief Technology Officer
LAB³

HOW CLOUD
READY ARE YOU?

What do you know about your on-premises estate today?

DIGITAL ESTATE RATIONALISATION

Digital estate rationalisation is the process of discovering, assessing and evaluating your existing applications, infrastructure and broader digital ecosystem. With the goal of discovering areas of focus or value to migrate workloads into cloud.

Cloud migration represents a significant transformation for any organisation, encompassing a broad spectrum of changes across, technology, people and culture. It can be a process fraught with complexity and potential pitfalls, if not carefully planned, measured and monitored.

Simply relocating applications and infrastructure from an on-premises hosted location to the cloud without a clear, tailored approach can negate any of the financial or operational advantages that the cloud offers.

To harness the full spectrum of benefits the cloud has to offer, it's crucial for organisations to devise an approach to cloud rationalisation that feeds into a wider cloud strategy. This rationalisation needs to be grounded in a comprehensive data-driven assessment that goes beyond mere technical considerations.

ASSESS

A holistic discovery and assessment of your technical estate is the first step to uncovering the value of cloud adoption for your organisation. A detailed inventory of the technical characteristics of each environment, including virtual machines, applications, utilisation, storage, and services.

This is typically achieved by conducting a data-driven assessment and is vital to understand for several reasons:

- **Identification of redundant infrastructure, outdated software, and underutilised resources.** This information can provide opportunities to streamline operations and realise significant cost savings.

- **Uncovering security vulnerabilities, compliance issues, and other risks associated with the estate.** Proactive measures to mitigate these risks can be incorporated into your plan.

- **Informing strategic decisions about IT investments, resource allocation, and transformation initiatives.** This ensures the organisation aligns plans for their IT infrastructure with their business objectives.

- **Providing the data to make informed decisions** about cloud foundations, migration strategy, operational management, vendor/partnering, staff and skills uplift, and much more.

- **Identify opportunities for modernisation and innovation, to help future-proof organisations**, ensuring they can stay competitive across a rapidly evolving digital landscape.

Getting a head start on Digital Estate Rationalisation

Digital estate rationalisation can be approached in several ways. The manual method involves systematically collecting data from an Inventory Management or Configuration Management Database (CMDB), and supplementing this with additional information gathered from IT personnel, application owners, and other stakeholders. While this approach provides a good starting point, it can be a labour-intensive process that's prone to human error, and introduces risk if your knowledge base is inaccurate or incomplete.

An alternative strategy is to leverage technology to thoroughly scan your digital estate and surface valuable insights. Dr Migrate is an advanced cloud migration tool designed to streamline and accelerate the process of migrating applications and infrastructure to Azure.

Built on top of Azure Migrate, this tool leverages AI and Machine Learning to automate many of the labour-intensive tasks associated with cloud migration.

Dr Migrate simplifies the collection of technical characteristics of the environment, including details about virtual machines, applications, databases, storage, and networking utilisation. It groups applications with associated infrastructure and maps their characteristics to Azure capabilities.

This process identifies optimisation opportunities in Azure and provides Total Cost of Ownership (TCO) projections for each option. It also highlights risks associated with end-of-life software and potential modernisation opportunities. Finally, it recommends 6R migration treatments and wave plans to prioritise the migration sequence.

ASSESS

Critical Activities

- **Identify Cost Savings and Efficiencies**
  Identify redundant infrastructure, outdated software, and underutilised resources to streamline operations and save costs.

- **Build a Strategic Plan that Mitigates Risk**
  Uncover security vulnerabilities and compliance issues to inform strategic IT investments and resource allocation.

- **Prioritise Migration and Modernisation Effort**
  Use tools such as Dr Migrate to map infrastructure to Azure, optimise costs, and prioritise migration and modernisation efforts.

How does cloud accelerate your strategic business outcomes?

PLAN

The planning stage is where the translation of your organisation's aspirational goals of cloud adoption turns into an actionable plan. Cloud adoption plans build on top of a well-defined strategy, which at a minimum should outline motivations, business outcomes and business justifications for cloud adoption. This enables a laser focus on the value provided by the cloud balanced by the effort required to realise them.

You will have your defined strategic inputs such as:

- Why are we adopting the cloud?
- What results do we expect to see from the adoption of the cloud?
- How will we measure success both technically and for the business?

You can now build your cloud adoption plan, which focuses on prioritising, rationalising and defining timelines for the scoped migration to the cloud. It is important to remember that as you make decisions on the outputs of the assessment phase, you continuously bring them back to the strategic outcomes of your organisation.

Where to start?

The planning phase of cloud adoption and its significance to the overall success is often undervalued. This phase is where tactical inputs such as skills readiness, organisational alignment and digital estate rationalisation are paired with more detailed requirements from wider teams.

Building on the discovery completed within the assess phase, leveraging tooling such as Dr Migrate, you should now have a complete inventory of your digital estate. It is now important to dive into the requirements of your technical teams to determine additional opportunities for tooling simplification and guiding principles for cloud adoption for your organisation.

One way to look at these requirements is through the 'ways of working' today in an on-premises world versus a cloud-native one. Platform capabilities and shared services such as backup, file storage, patching, identity management, monitoring, DNS, networking and much more are now opportunities for simplification and centralisation in determined tooling.

Once business motivations, technology drivers and tooling preferences are aligned, early opportunities to consolidate existing on-premises services with cloud-native alternatives start to become clear, reducing the migratable footprint and providing a more accurate basis with which to determine service consumption and costs in the cloud.

PLAN

Critical Activities

- **Align Technical Goals to Business Drivers**
  Define clear technical drivers and align to business drivers to guide the migration, such as datacentre exit dates or hardware renewal cycles.

- **Determine Service Requirements and Tooling Preferences**
  Consider platform-wide service needs and tooling preferences for cloud operations, identifying opportunities to modernise ways of working.

- **Align Planning with Business and Technical Requirements**
  Consolidate on-premises services with cloud-native alternatives to reduce the migratable footprint and align cloud adoption planning with business and technical requirements.

Have you rationalised your on-premises estate against cloud native solutions?
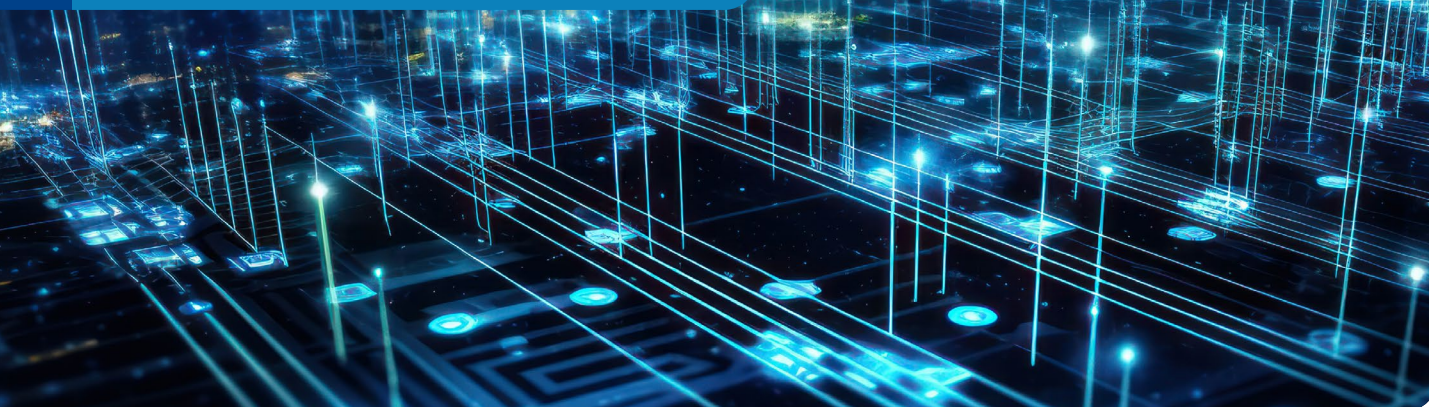
CLOUD RATIONALISATION

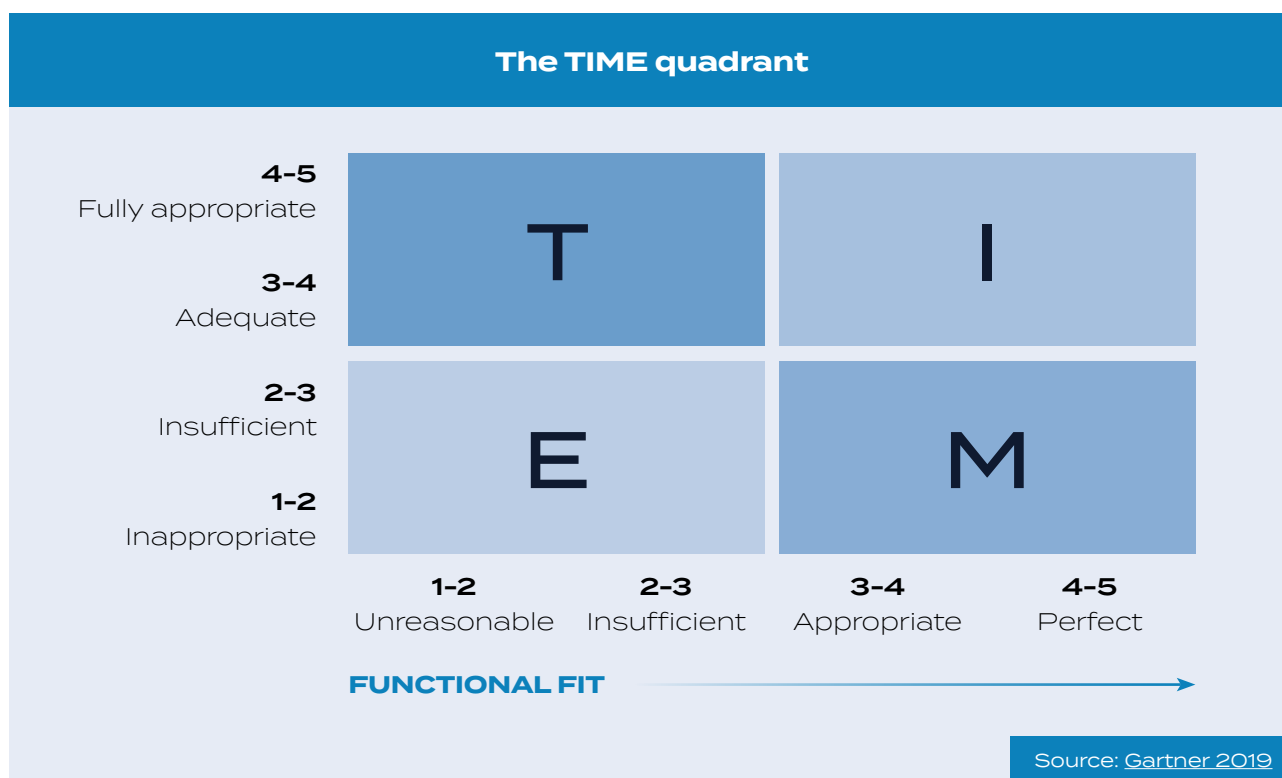As you embark on your cloud adoption journey with the imminent launch of the New Zealand North region, arguably the most critical stage within your cloud adoption plan is the prioritisation, rationalisation and timelines surrounding the treatment and migration of each workload or application.

Dr Migrate provides a head start on this leveraging its algorithms to suggest recommendations based on native services and the discovered services and applications. However, the rationalisation process is about ensuring your business objectives and drivers are considered alongside the recommendations to provide a holistic view of savings and TCO of Azure for your organisation.

To achieve this LAB[3] leverages Gartner's TIME (Tolerate, Invest, Migrate and Eliminate) framework, an industry-standard framework for maximising the business value of your application portfolio. It achieves this by grouping applications in your portfolio into quadrants based on their technical and functional fit across your organisation.

Technical fit refers to the quality of the application. Functional fit relates to how well the application aligns and serves business capabilities and processes.

- Applications with high technical fit but low functional fit are **tolerated**

- Applications with high technical fit and high functional fit are **invested** in

- Applications with low technical fit and high functional fit are **migrated**

- Applications with low technical fit and low function fit are **eliminated**

The TIME quadrant

4-5 Fully appropriate		T	I
3-4 Adequate			
2-3 Insufficient		E	M
1-2 Inappropriate			
	1-2 Unreasonable	**2-3** Insufficient	**3-4** Appropriate	**4-5** Perfect

FUNCTIONAL FIT →

Source: Gartner 2019

The TIME framework helps drive discussions and decision making about the application's lifecycle within your organisation. This is an important step to clarify the immediate and future business requirements for each application to inform their rationalisation.

As each application progresses through this stage of the planning process for cloud adoption it is important to consistently revisit key innovation indicators, including:

- Do the applications in this workload create market differentiation?
- Does the data within this application enable new products or service offerings?
- Does the business already have investment for this application set aside?

Where the answer to the above question is 'yes', rearchitecture should be considered over migrating the application as-is.

Quick wins can still be achieved even if applications may be on the future roadmap for innovation. Key migration indicators include:

- Is the application's source code stable?
- Is cost reduction associated with this workload?
- Is reduction of operational complexity a goal for this workload?
- Are there security concerns or is the workload end of life?

Using the TIME framework LAB³ accelerates and optimises planning efforts by focusing on the value-add applications where cloud solutions are feasible and cost-effective for your specific scenarios. Using Dr Migrate and our international expertise the output of the TIME framework can often be useful later in your migration efforts when technical discussions need to be refocused on business value.

Application Treatment – The 6R's

The output of the TIME framework provides you with a complete list of your estate and a prioritised understanding of each application's functional and technical fit against your organisation's strategic objectives.

Originally coined by Gartner in 2010, "The R's Model", refers to a set of treatment options in cloud adoption dependent on the phase of the applications lifecycle. LAB[3] have standardised on the 6R's described below.

THE 6R MODEL

1	2	3	4	5	6
REHOST	RE-PLATFORM	RE-ARCHITECT	REPLACE	RETAIN	RETIRE
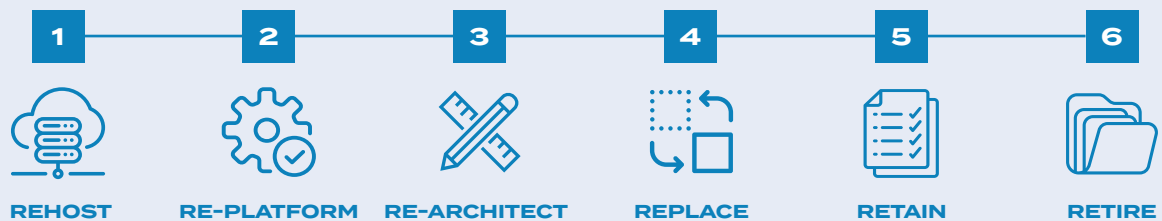
1

REHOST

Rehosting involves moving applications directly to Azure with minimal changes. This approach is often chosen for its speed. Minimising effort whilst maximising value.

Example: Migration of a Server from Hyper-V or VMware to an Azure Virtual Machine.

2

RE-PLATFORM

Re-platforming involves making some optimisations during migration to maximise the advantage provide by PaaS services within Azure, without changing the core architecture of the application.

Example: Moving an IIS Web Application to an Azure App Service, usually also done in conjunction with a migration of the data of the application from an on-premises SQL Server to an Azure SQL Database or SQL Managed Instance.

3

RE-ARCHITECT

This treatment involved the modification and optimisation of the application to fully leverage cloud-native capabilities within Azure. This typically involves significant changes to the application's architecture and infrastructure to improve scalability, performance, and resilience.

Example: Transforming a monolithic application into a set of microservices deployed on Azure Kubernetes Service (AKS) or Azure Container Apps, perhaps also leveraging Azure Functions for supplementary services.

4

REPLACE
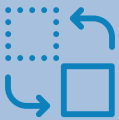
Migrating from an existing application to a new Software as a Service (SaaS) based or Commercial Off The Shelf (COTS) product. Suitable when an existing application cannot meet business requirements and a more efficient cloud-based solution is available in market.

Example: Replacing Exchange 2008 with Microsoft 365 enabling Exchange Online and SharePoint Online. Whilst there is still a migration required in terms of application data the services are managed by a provider, in this example Microsoft.

5

RETAIN

Retaining involves keeping certain applications or components within their current environment, such as remaining on-premises. This maybe due to compliance or business policy objectives.

Example: Deciding to keep a legacy financial system on-premises Hyper-V environment to address regulatory constraints. Whilst updating the operational tooling with Azure Arc to modernise and reduce operational complexity. (See Arc section)

6

RETIRE

Decommissioning outdated or now redundant applications or systems that are no longer required by your business.

Example: Legacy backup solution is no longer required after modernising to Azure Backup and Azure Site Recovery. The old tape-based backup solution can be decommissioned.

While every organisation's cloud journey is unique, LAB³'s migration approach leveraging 6R recommendations and the TIME Framework has helped hundreds of organisations accelerate time to value for their cloud investment. We're ready to guide you with a clear, actionable plan that aligns to your organisation's objectives, investment and timeframes.

RATIONALISATION

Critical Activities

- **Rationalise Applications with TIME Model**
  Use Gartner's TIME model to align IT portfolio plans with business objectives, categorising applications based on their business value and technical quality.

- **Prioritise Applications Before 6R Assignment**
  Group applications into Tolerate, Invest, Migrate and Eliminate quadrants to determine immediate and future business requirements and focus efforts accordingly.

- **Optimise Planning and Decision Making**
  Use the TIME mapping exercise to provide decision–making criteria for effective planning and migration.

Does your strategy align to your business case?

BUSINESS CASE

Having invested the time and resources to go through detailed assessment, planning and cloud rationalisation phases of migration planning, it's time to translate the culmination of these efforts into a clear business case.

The business case is your opportunity to reflect against the data points collected and the original strategic intent and look to update the strategy where relevant, but also to paint a holistic picture of the true cost and opportunities that come with moving forward with cloud adoption in the New Zealand North region.

At LAB³, business cases are developed with data points collected from a Dr Migrate assessment. This data helps create a deeper understanding of the true cost of cloud migration. We also incorporate **overarching architectural principles** that drive decision-making and contribute to the Total Cost of Ownership (TCO).

Whilst Dr Migrate doesn't write the business case holistic, it gives unrivalled insights into server migration readiness, application modernisation, right-sizing and a customisable wave plan based on network affinity and dependencies.

These insights help to highlight key elements of your business case and where value can be demonstrated through the adoption of Microsoft Azure.

It is important when drafting your business case for cloud migration to have supporting data points such as:

- A clear inventory and understanding of the current digital estate, with identified opportunities for cost savings and modernisation.

- Business drivers and technical requirements that align IT infrastructure plans with organisational goals.

- Strategic decisions on IT investments, resource allocation, and digital transformation initiatives based on data-driven assessments.

- A roadmap for migration with detailed wave plans (including first mover candidates, required resources, timelines, dependencies, and potential risks).

- Financial projections and cost optimisations that build a strong case for cloud migration, showcasing the value and ROI of the move to Azure, alongside labour costs.

Critical Activities

- **Confirm Migration Roadmap and Financial Projections**
Finalise the migration roadmap with wave plans, including resource requirements, timelines, risks, and dependencies. Ensure the roadmap aligns with business priorities, leveraging financial projections and cost optimisations to clearly demonstrate the value of cloud migration. Consider both capital and operational expenses and build a flexible model to accommodate future growth and evolving business needs.

- **Understand TCO Prediction**
Documented Total Cost of Ownership for Cloud, incorporating sensitivity analysis to account for potential over or underspend based on architectural choices and scaling strategies. TCO should cover not just immediate migration costs but also operational savings, long-term infrastructure scaling, and potential business disruptions during migration.

- **Review Strategy Alignment**
Ensure that your cloud strategy is still aligned, integrated with key date points from the assessments and planning stages, holistically supported by the overall business objectives. This alignment should link technical execution with broader organisation goals such as scalability, innovation and enhanced customer experiences, creating a unified vision between business leadership and technology solutions.

- **Engage Stakeholders**
Ensure that key stakeholders, including executives and department heads, are aligned with the business case, understanding both the strategic and financial rationale behind the migration. Engage stakeholders early and frequently to ensure their support throughout the process.

CLOUD FOUNDATIONS & LANDING ZONES

With a clear understanding of your digital estate and potential treatments for each workload that maximise the benefits of your transformation; there are two distinct scenarios to navigate, greenfield and brownfield, when deploying cloud infrastructure.

Which field is most fertile for your workloads?

GREENFIELD

Greenfield deployments are a unique opportunity to design your underlying cloud foundations with a clean slate. This enables the most direct alignment to frameworks such as Microsoft's Cloud Adoption Framework, and other cloud-native architectures and patterns.

In the context of the New Zealand North region as your 'primary' region, this would mean aligning with the architecture capabilities of the region. Asking questions such as:

- What are your timelines?
- Which services will you use?
- What are your Disaster Recovery requirements?
- What are your High Availability requirements?
- Will you require multi-region connectivity?

These questions help to ensure you can leverage the NZ North region in an effective and timely manner as the services ramp up.

BROWNFIELD

Brownfield deployments, on the other hand, can present unique challenges. In the context of NZ North, serving two key scenarios; Multi-Region and Repatriation. Brownfields deals with the extension or integration of a new region into existing operational practices, tooling, ways of working and governance policies.

Unique challenges can present themselves with this approach due to differences in region capabilities, as well as the technical debt of the existing foundational platform. In brownfield scenarios it is important to ask yourselves the below questions:

- What are your motivations, are they legal / regulatory based or performance-driven?
- Is repatriation a good chance to resolve outstanding technical debt or make additional improvements?
- Does a new region with global routing remove the need for repatriation?

These questions can help expose important conversations that drive organisational alignment and focus effort on the value-adding capabilities of a brownfield expansion.

Whether you are pursuing a greenfield deployment of Azure for the first time or modernising a brownfield environment by extending into NZ North, the importance of a solid Cloud Foundation and well-architected Landing Zone cannot be overstated. These core components such as network, identity and DevOps tooling such as IaC (Infrastructure as Code) enable organisations like yours to build resilient, secure, and scalable environments that can adapt to changing business needs.

NETWORKING

A critical foundational element when it comes to cloud landing zones, networking plays a central role in ensuring the security, scalability, performance and overall success of cloud environments.

Traditionally, networking is quite a siloed capability within an organisation and the adoption of cloud capability often exposes the requirement for more of a shared function when it comes to networking. This siloed capability is often established with the belief of protecting the business' crown jewels within a DMZ (Demilitarised Zone). However, cloud lends itself towards Zero Trust architectural principles which represents a shift in the treatment of networks.

Zero Trust Architecture

Cloud redefines a broader boundary, whereby no traffic is trusted by default whether it originates from within or outside the organisation's networks. This means that security controls are required to be applied at every layer, to ensure continuous verification and monitoring of traffic.

The boundary fundamentally shifts from a trusted network range to one based on security. Entra (formerly Azure Active Directory) plays a crucial role in this, but we will cover this in more detail within the Identity section.

Unlike the former monolithic perimeter of on-premises networks, cloud networking is grounded in the micro-segmentation of the network. Applying security controls at multiple levels, such as the subnet, virtual network or even per a specific cloud resource. This micro-segmentation helps limit lateral movement within networks and protects against breaches within a specific layer of the network.

Zero Trust Architecture enhances security whilst also enabling greater agility in modern cloud environments. By continuously verifying identities, enforcing least-privilege access and implementing strict controls across every layer of the network, there is a minimised attack surface with greater visibility if the foundational elements are established correctly.

Network Topologies

As micro-segmentation becomes the norm in cloud networking, traditionally aligned topologies have been increasingly questioned due to the high operational overhead associated with managing cloud networks using legacy on-premises methods. The shift to the cloud has exposed the limitations of these conventional approaches, emphasising the need for more dynamic and automated solutions that better align with the cloud's flexibility and scalability.

Hub-and-spoke topologies have been a widely adopted network architecture in Azure, where a central hub VNet (Virtual Network) connects to multiple spoke VNets, enabling centralised control over traffic flow, security, and connectivity. This model has proven effective for many organisations; however, it can introduce significant challenges in larger, complex environments and organisations.

The primary issue lies in the operational complexity; as the number of spokes increases, managing peering relationships, security policies, and routing configurations can become cumbersome and prone to error. Additionally, traffic between spokes must often route through the hub, which can lead to increased latency and bottlenecks, especially in multi-region deployments.

More recently, Azure Virtual WAN (vWAN) offers a more streamlined and scalable solution by providing a global transit network that automatically manages connectivity and routing between regions, branches and on-premises environments. With vWAN organisations benefit from dynamic routing without missing out on centralised security management.

This can drastically reduce operational overhead associated with the manual configuration of hub-and-spoke topologies whilst also improving performance by ensuring traffic is routed through the most efficient paths.

When it comes to enabling your organisation on the critical foundational element of networking, it's crucial to consider the complexity of your requirements and future growth and scale plans. By aligning your network topology and architecture with your long-term goals, you can prevent potential pitfalls such as limited flexibility, and the accumulation of significant technical debt.

It's important to recognise that you aren't required to build everything from Day 1, starting with a well-planned network architecture that can grow along with your infrastructure allows you to build confidently whilst minimising operational overhead and enabling seamless scale.

IDENTITY

Identity and its management are a cornerstone of your cloud landing zones, acting as the foundation upon which scalable and compliant environments are built. In a cloud-first world where traditional identity perimeters no longer exist, as we mentioned in the previous section, identity becomes the primary security boundary.

Historically speaking identity has been somewhat of a siloed function within organisations, often managed by a single team or department. However, as your organisation expands into the cloud this approach is no longer sustainable. In environments such as Azure, identity management must be a shared responsibility, tightly integrated alongside other core functions, security, networking, infrastructure, and development workflows.

With such a fundamental shift in how identity is managed and implemented as organisations transition to the cloud, it becomes essential to explore models and methods that can accelerate the design of these new security boundaries. At LAB[3], we advocate for a persona-driven approach as a core strategy for defining roles and responsibilities that shape teams' workflows.

This approach not only streamlines identity management by tailoring access controls to specific personas but also reinforces a least-privilege access model. By focusing on personas, organisations can ensure that users are granted the minimum level of access required to perform their day-to-day tasks, significantly reducing security risks and operational overhead while aligning with the overall cloud strategy.

Microsoft Entra (Previously known as AAD, Azure Active Directory), which serves as the foundational capability for managing identity, access, and security. Entra provides several critical features that support a persona-driven least privilege access model, including the use of Role-Based Access Control (RBAC), Conditional Access, Privileged Identity Management (PIM) and Entitlement Management.

These capabilities within Entra allow your organisation to implement fine-grained access controls that can be specific to people, workflows, and outcomes without adding to the operational overhead of traditional AD management.

DID YOU KNOW?

Persona-driven access models help to define key roles and responsibilities as well as where the requirement for tooling such as PIM (Privileged Identity Management) can be used.

RBAC (Role-Based Access Control)

RBAC is a method of managing access to resources by assigning roles to users based on their job functions or responsibilities. It aims to ensure that users only have the permissions needed to perform their day-to-day tasks.

Conditional Access

Conditional Access policies in Entra enable dynamic access controls based on specific conditions, such as user identity, location, device health, and behaviour. These policies help enforce security by granting or restricting access to resources automatically based on the context of each access request.

PIM (Privileged Identity Management)

PIM is a feature within Entra that provides just-in-time access to higher privilege roles, ensuring that elevated permissions are only granted when needed and for a specified duration. PIM also facilitates approvals via specific users for specific roles, as well as generates audit logs for a SOC to monitor.

Access Packages

A key feature within Entra's Entitlement Management, Access Packages enables organisations to group access to various resources and types of resources, such as applications, AD Groups, and SharePoint sites, all into a single, requestable package. These packages are then managed through governed workflows, making it easier to manage permissions across your different personas and ensuring access is granted in a controlled and consistent manner.

In our experience, Access Packages are one of the most underutilised features within Entra, despite their potential to significantly reduce the operational burden of managing user access. The straightforward design and implementation streamline the process of provisioning, auditing, granting, and revoking access, allowing your teams to automate complex access management scenarios while maintaining security and compliance standards.

Service Principals

Service Principals can compare to Service Accounts in traditional Active Directory. They represent an identity created specifically for applications, services, or automated tools to interact with Azure resources.

In simple terms, Service Principals serve as the identity for non-human identities, enabling them to authenticate and access Azure resources as needed.

Widely used in DevOps workflows and CI/CD pipelines, Service Principals help enforce a least-privilege access model by restricting higher-level permissions to these non-user based accounts. Ensuring that automation processes operate securely without overexposure to sensitive permissions and enabling a separation of duty from human-based accounts.

As you can see identity in Azure Landing Zones serve as a foundation for security, scalability and enablement in cloud environments. Modern identity management requires a shared responsibility model integrated with security, networking and development workflows. As your organisation looks to adopt the new NZ North region of Azure it is important to ensure you look to define or extend the best practice approaches mentioned above to maximise the capability without sacrifice of compliance and controls.

PLATFORM AUTOMATION & DEVOPS

As organisations such as yours look to the new NZ North region to define or expand their existing cloud capability, it is a perfect opportunity to assess or plan the level of platform automation and DevOps practices for your organisation to adopt. These practices are not just technical enhancements; they are key to creating a resilient, controlled and scalable cloud environment that drives the maximum return on investment for your organisation.

Platform Automation is vital to consistently manage and maintain your cloud platform and infrastructure. By automating not only the deployment and configurations of your resources but also the guardrails, policies, RBAC models etc. your organisation can ensure the best practices are adhered to consistently.

Often overlooked but of critical importance is the relevance of ensuring that comprehensive standards around Day 2 Operations are defined and baked into your platform's automation capabilities. Most organisations see an immediate benefit of the cloud through the rapid provisioning and scaling of resources, whilst leaving the operational activities such as ongoing management, patching, monitoring and optimisation of the platform and services deployed.

Tooling such as Hashicorp Terraform is invaluable in this regard, as it allows you to define not only your infrastructure as code but also platforms such as Databricks, GitHub, Azure DevOps and thousands more. The use of Terraform enables the ability to have version-controlled, repeatable, and auditable deployments. LAB[3] is a hyper-specialised HashiCorp partner and has extensive experience in leveraging Terraform to deploy and manage Cloud Foundations on Azure.

In tandem, DevOps practices provide the framework for Continuous Integration and Continuous Delivery (CI/CD), enabling your organisation's platform teams and developers to be more effective and efficient through collaboration.

This is a large culture shift; changing from the risk-averse, people-driven, manual processes of On-Premises environments to a code-driven and automated process, where responsibility is shared rather than siloed. This shift breaks down silos and fosters a shared responsibility model for delivering value at speed.

In addition to Terraform platforms such as GitHub or Azure DevOps play a crucial role, serving as the centralised platform for code collaboration, version control and CI/CD pipelines. Both GitHub and Azure DevOps are platforms that enhance collaboration, streamline code management, and integrate security into the development lifecycle. With tooling such as GitHub Copilot and GHAS (GitHub Advanced Security), AI and automation enable teams to work more efficiently together whilst embedding security checks early in the process.

Whether your organisation is venturing to the cloud for the first time or simply expanding its footprint by adding NZ North as a region through new platforms and tooling. Training and upskilling of your teams is crucial to hitting the ground running. These new practices of platform automation and DevOps represent a change in the tooling used in day-to-day work and a cultural shift within your teams. Spending time to map out the new roles and responsibilities of teams across a shared responsibility model as part of a new operating model is a key hurdle to unlocking the value presented by Azure.

THE LAB³ LANDING ZONE ACCELERATOR – BEDROCK

At LAB³, we have deployed LZ (Landing Zones) and automation solutions for the largest and most secure organisations across Australia and New Zealand. Our LZ accelerator focuses on rapidly enabling a secure and scalable footprint through opinionated automation building blocks, written in HashiCorp's Terraform, to accelerate the adoption of the cloud for your organisation.

Aligned to the core principles of the Microsoft CAF (Cloud Adoption Framework), our solution builds your organisation's cloud foundation on years of experience and successful implementations across FSI and Government clients.

We look to partner deeply with your organisation to define, document and deploy your ideal starting point for cloud adoption, whilst providing complete solutions for the Day 2 tasks such as patching, onboarding, and deployments of applications into your new landing zones.

To achieve this, we come to all projects with opinionated architecture that prompts informed decisions aligned to your organisation's scalability, operational and security requirements for the following pillars:

ACCELERATED LANDING ZONE ONBOARDING	By implementing a well-structured, stateful managed automation platform, you can onboard secure application landing zones in a matter of minutes.
LAYERED SECURITY	Using Azure Virtual WAN to provide a hub-and-spoke networking architecture takes care of micro-segmentation and network security while features like Privileged Identity Management (PIM) and a well-defined Role Based Access Control (RBAC) take care of least privilege and just-in-time access.
COST MANAGEMENT	Extending beyond Microsoft's CAF, providing Virtual Machine Power Management capabilities to ensure your dev/test workloads are powered off when not utilised.
BUILT-IN POLICY ENGINE	Managing Azure Policy as code enables consistent, automated deployment and enforcement of governance policies across your cloud environment, ensuring compliance and reducing manual errors.

FIND OUT MORE

Get in touch to discuss how these pillars align with your requirements, or to see a demonstration of our automated Landing Zone Accelerator capability.

CLOUD MATURITY ASSESSMENT

For those who have an established cloud capability on Azure but want to understand how they align to best practices, where potential areas of improvement exist such as cost saving, security, or automation capabilities. LAB³ have a Cloud Maturity Assessment capability, which is built through a two-phase approach.

PHASE 1

Firstly, we review your existing Azure implementation to identify opportunities where the platform and services can do more heavy lifting, without taking your teams away from their day-to-day work.

This review enables us to ask focused questions to better understand your operations and pain points when we do sit down with your teams.

PHASE 2

We then hold a series of workshops with your teams focused on the identified opportunities.

The intent of these workshops is to uncover previous decisions made and curate a backlog of tasks to uplift the maturity of Azure based on the requirements of your organisation.

This assessment is a full 360-degree look at all foundational elements such as Identity, Networking, Automation, Naming, etc of your implementation of Landing Zones on Azure.

FIND OUT MORE

Contact us to schedule your Cloud Maturity Assessment and unlock the full value of your Azure investment.

HYBRID CLOUD OPERATIONS

At LAB³ we have a unique way of approaching Hybrid environments. As a born-in-the-cloud Microsoft Partner, we look at how best to leverage modern technologies available to us to bring a "Cloud Down" discipline to your existing environments on-premises, rather than extend the legacy environment and solutions from "On-prem Up."

This approach extends the power and flexibility of Azure into your existing on-premises environments. This provides the full capabilities of Azure, regardless of where your data and compute resources reside, delivering a seamless and consistent experience across all environments, whilst also modernising your operational processes and upskilling your teams.

Now that you have a solid Azure cloud foundation leveraging LAB³'s Landing Zone accelerator, or a path to Azure improvements through our assessment – your organisation is perfectly positioned to extend these foundations to your existing on-premises environments via Azure Arc.

AZURE ARC

Microsoft Azure Arc is the key enabling component for LAB³'s "Cloud Down" approach to Hybrid and & Edge environments. Azure Arc, establishes a bridge between your on-premises environments to Azure's security, management, and governance capabilities, resulting in a unified hybrid environment that operates under the same principles and with the same tooling as your cloud-native resources within Azure.

Azure Arc simplifies your overall IT Operations through the unification of management of on-premises, multi-cloud environments under a single, consistent framework using Azure's native toolset. This standardisation means that instead of relying on a mix of third-party solutions to manage disparate environments, your organisation can now leverage Azure's integrated suite of tools for monitoring, security, and governance across your compute environments.

Leveraging this approach can lead to a reduction in cost, not only through the elimination of multiple third-party software products but also through the streamlining of your operations. Rather than having multiple tools glued together with scripts, bespoke automation, and critical knowledge sitting with individual engineers within your teams.

With Azure Arc the divide between Azure and on-premises operational environments is bridged, allowing for a single team to manage both environments within its' unified approach. This convergence reduces the complexity and overhead associated with maintaining separate teams and tools for different environments, leading to more efficient operations and an overall more cohesive IT strategy.

In addition to the operational efficiencies gained, Azure Arc plays a pivotal role in providing your organisation with ESUs (Extended Security Updates), for infrastructure that has reached its EOL (End-of-Life). This last resort is for the support of legacy infrastructure and whilst not intended as a long-term solution, or to extend the product's lifecycle or technical support, it does provide a temporary bridge to stay secure whilst planning your migration to newer, supported systems.

Systems that are connected through Azure Arc become eligible to receive the same extended security benefits that are afforded to the native Azure resources. This capability is incredibly valuable for your organisation if your critical workloads are running on older infrastructure due to compliance or application dependencies.

Azure Arc not only provides a single pane of glass in which to manage your entire infrastructure capability, it also provides a unified toolset to reduce the overall cost of managing your infrastructure whilst also providing extended security updates to critical systems running on legacy infrastructure.

AZURE STACK

Whilst Azure Arc extends Azure's management and security capabilities to existing on-premises and multi-cloud environments. Azure Stack's portfolio brings Azure's cloud infrastructure directly into your data centre. Azure Stacks' portfolio is comprised of three solutions, Azure Stack Hub, Azure Stack HCI (Hyper-Converged Infrastructure), and Azure Stack Edge, however at LAB[3], we focus on the use of Azure Stack HCI.

Azure Stack HCI

A complete hybrid cloud solution, Azure Stack HCI, is designed to modernise on-premises data centres by combining virtualised workloads with cloud-based management, security, and services.

It enables your organisation to run virtual machines, containers, and storage-intensive applications on-premises. Usually paired with Azure Arc to provide a single point of management across your modernised hybrid environment Azure Stack HCI is a great solution when looking to replace aging server infrastructure with a modern, scalable, and high-performing platform.

A perfect solution where branches or remote offices are a part of your organisation's architecture, it provides local compute and storage with connectivity to Azure for centralised management, monitoring and patching.

Azure Stack HCI offers a holistic approach to solving traditional problems associated with hybrid compute environments. LAB[3] has recently seen a large uptick in interest specifically around the use of Azure Stack HCI with its ability to modernise an existing on-premises estate through the process of a hardware refresh or for use in modern retail environments.

Azure's Stack HCI can be an enabling first step to the use of cloud technologies in your organisation or an extension to your new NZ North region Landing Zones. As a physical asset that is deployed within your data centre or other locations such as a branch office or retail storefront, your organisation can enable capitalisation of the asset. This capitalisation (CAPEX) approach enables you to extend your cloud footprint without levering the sometimes harder-to-consume operational budget (OPEX) usually associated with cloud workloads and adoption.

DID YOU KNOW?

Azure's Stack HCI can be leveraged to capitalise physical, on-site assets? **Get in touch** to find out how LAB[3] have helped clients capitalise assets and free up operational budgets.

HYBRID LANDING ZONE

Armed with the knowledge of the Hybrid estate at Microsoft through Azure Stack and Azure Arc, it's clear that success of the solutions within a portfolio requires an established, secure and strong landing zone foundation. This is heightened when you consider the rolling introduction of Azure services to the NZ North region over the first 90 days of GA (General Availability). A well-architected landing zone serves as the foundation layer that supports all cloud and hybrid operations, ensuring that your organisation can fully capitalise on the capabilities of the NZ North region as they come online. The extension of your Azure Landing Zone to enable and maximise the value of Azure Arc and/or Azure Stack HCI are the below two key elements:

- **Hybrid and Multicloud connectivity:** Understand and Implement key network design considerations to enable Azure Arc

- **Unified Operations:** Include Azure Arc-enabled resources to extend your governance and operations support with consistent tooling.

- **Identity & Access Management:** Plan for the standardisation or centralisation of your organisational user identity.

The value provided to your hybrid estate through a solid landing zone is amplified when both your hybrid and cloud estates are driven through automation and a code-driven solution. **LAB³'s Landing Zone Accelerator Bedrock** is the quickest way to define a greenfield platform with high levels of automation for both deployment and Day 2 operations of cloud and hybrid resources.

By extending your implementation of Bedrock into a hybrid on-premises environment the acceleration uplifts the reliability, efficiency, and security posture of your legacy environments through a well-structured and centralised management capability.

Workload Selection

When it comes to incorporating a solution such as Azure Stack HCI into your environment, careful consideration is required when determining which applications are best suited for this solution.

As mentioned, Azure Stack HCI is ideal for workloads that demand high performance, low latency and data processing capabilities, such examples are:
- Virtual Desktop Infrastructure
- SQL Server Database
- Retail, Branch or Remote Office Locations

To make informed decisions on which workloads to deploy to Azure Stack HCI, the use of tooling such as **Dr Migrate** which integrates **Gartner's TIME** (Tolerate, Invest, Migrate, Eliminate) framework is critical to maximising return on investment.

At LAB³ we take an innovative approach to Hybrid and Edge Cloud Operations leveraging the full potential of Azure Stack and Azure Arc to bring the power of Azure directly into your on-premises and edge environments. By focusing on our "Cloud Down" approach we can enable a seamless flow from your NZ North region Landing Zone into your hybrid environments, providing consistent security, management, and operational efficiency across all platforms.

Such an approach enables new capabilities to be explored by your business such as the concept of a modern store, leveraging Azure Stack HCI, by running AI models at the edge to unlock new business, or repurposing idle compute without increasing operational cost. Through a "Cloud Down" approach underpinned by a solid landing zone foundation, unlocking new capabilities does not come in the form of regrettable spending.

VALUE REALISATION

The launch of the NZ North region marks a pivotal moment for Aotearoa-based organisations, which will have access to a fully featured hyperscaler cloud for the first time. By adopting Azure's latest region, businesses gain access to cutting-edge technologies, enhanced performance and local data residency, which can be critical for meeting both operational and regulatory requirements.

The NZ North region not only offers advanced cloud infrastructure tailored to the unique needs of New Zealand organisations but also unlocks new opportunities for innovation and growth. With this strategic adoption, companies can accelerate their digital transformation, optimise costs, and scale their operations seamlessly, setting the stage for long-term success in an increasingly competitive landscape.

AZURE OPENAI SERVICE

Since becoming generally available in January of 2023, Azure OpenAI Service has taken the world by storm as the leading AI development platform in the world. Azure OpenAI enables organisations to harness the capabilities of generative AI, empowering them to automate complex processes, generate high-quality content, and dive deeper into insights from data, all with less human involvement and effort.

This integration of AI into business operations not only enhances productivity but also significant competitive advantages, allowing your organisation to stay ahead in a rapidly evolving digital landscape.

Azure's OpenAI Service is designed to cater to a wide range of use cases, from developing sophisticated natural language processing applications to creating interactive, multimodal AI experiences that integrate text, image, and audio.

Importantly core to Azure's OpenAI Service is its commitment to content safety. As organisations, such as yours look to deploy AI-driven applications, ensuring that the systems generate safe and appropriate content is paramount. Azure OpenAI includes content moderation tooling that helps organisations enforce compliance within defined guard-rails and ethical guidelines.

The ability to integrate Azure's OpenAI Service with Retrieval-Augmented Generation (RAG) allows your organisation to ground AI models to your specific data. This capability when interacting with vast amounts of data, provides more accurate and contextually relevant outputs, therefore increasing the value of the output and potential automation outcomes.

LAB[3] is a leading partner within Microsoft's AI Cloud Partner Program and has recently announced an MoU (Memorandum of Understanding) with Microsoft to build an AI Centre of Excellence.

Recently partnering with Clayton Utz and subject of **a recent feature in The Australian** on the benefits of adopting AI. We have a unique accelerator that deploys secure, scalable Azure's OpenAI Services, allowing for rapid development of use cases and shorter time to value.

DID YOU KNOW?

LAB[3] has helped clients in highly regulated industries to prepare for and adopt Generative AI in their operations. **Get in contact** to learn more about our current AI offers.

FABRIC DATA PLATFORM

As organisations embrace the capabilities of the NZ North region, Microsoft Fabric stands out as a transformative platform for those looking to revolutionise their data and analytics strategies. The adage "garbage in, garbage out" underscores the importance of managing data quality, and Microsoft Fabric addresses this by providing a unified data platform that enables seamless integration of data from multiple sources and centralises data engineering capabilities in a single location.

Fabric is designed to tackle the challenges of modern data environments, where data is often siloed across various platforms and locations. Fabric's centralised data model empowers users from different departments to access and work with the same data sets, fostering a culture of collaboration and ensuring consistency across the organisation. This unified approach to data management breaks down silos, allowing for more cohesive and accurate insights.

Consolidating a range of Azure data services and third-party tools into a comprehensive end-to-end analytics and data platform. Fabric includes capabilities for data movement, processing, ingestion, transformation, real-time event routing, and report building. As a SaaS (Software as a Service) offering, Fabric centralises services such as Data Engineering, Data Factory, Data Science, Real-Time Analytics, Data Warehousing, and Databases, simplifying the management of complex data workflows.

The centralisation of data capabilities within Fabric drives collaboration and also enhances the security and quality of your data. This includes advanced features for identity and access management, dynamic data masking, and data classification.

Microsoft Fabric dismantles data silos, streamlines data workflows, and simplifies data governance, making it an important tool for organisations aiming to leverage data as a strategic asset.

AZURE VMWARE SOLUTION (AVS)

Azure VMware Solution (AVS) is Microsoft's solution that enables businesses to migrate their VMware workloads to Azure without the need for re-factoring applications or upskilling IT teams. AVS leverages native VMware technologies such as vSphere to transition virtual machines to a consistent VMware environment in Azure that is fully managed by Microsoft.

Broadcom's acquisition of VMware and their subsequent changes to VMWare licensing model, have provided more of an incentive to consider AVS as part of your migration strategy. With VMware shifting to a subscription-based per-core model, organisations may face significantly higher licensing costs at their next renewal. In this context, AVS provides an option to help avoid the potential financial impacts while facilitating a rapid exit from on-premises datacentres at a velocity that is typically much quicker than direct to cloud native workload migration.

Azure offers cloud benefits such as Reserved Instance pricing for AVS. This consumption model enables organisations to lock in their pricing for a term (typically 1 or 3 years), at a discount and remain protected from further price fluctuation while focussing on moving workloads to Azure cloud native services. In addition, through the Extended Security Updates (ESU's) benefit, companies can extend the support lifespan of legacy workloads once in Azure accessing Security and Critical updates providing further risk mitigation.

LAB³'s recommended adoption approach to AVS is executed over two main phases:

Rapid Migration to AVS:

Using Dr Migrate, optimal AVS configuration and TCO is identified before on-premises VMWare infrastructure is connected to AVS and rapid migration of workloads take place. Migration is completed in waves, at a benchmark velocity of up to 125 servers per week. Concurrently, modernisation planning begins at this stage which is based on assigning workloads with a **6R treatment**.

Cloud-Native Modernisation:

After AVS migration, LAB³ commences modernisation of workloads to Azure-native services based on modernisation treatments that were defined in stage 1. The typical strategy is to modernise systems that have Azure-based solutions such as:

- Migrating SQL Server to SQL Managed Instances.
- Modernising file services with SharePoint Online.
- Virtualising desktops with Azure Virtual Desktop.
- Consolidating observability and protection with Azure Monitor and Microsoft Sentinel.

DID YOU KNOW?

Azure VMware Solution (AVS) uses the same hypervisor, guest tools, and operating procedures as your existing VMware environment. This means there is no need for resizing or IP changes, and live migration can typically be achieved through VMware replication technology with minimal disruption.

DAFF TAKES FARMING DIGITAL

Australia's Department of Agriculture, Fisheries and Forestry partnered with LAB³ to enhance cloud infrastructure and enable automated provisioning of robust, scalable and secure services.

WATCH VIDEO

CRAIGS® INVESTMENT PARTNERS

LEAPFROG 2 YEARS ON CLOUD TRANSFORMATION TIMELINE

"The number one reason Craigs invested in Dr Migrate was visibility. We needed to gain a clear view over our technical estate, and to be able to present this not just to our technical team but at a management level as well."

DAVID JONES

Head of Technology
Craigs Investment Partners

2 YEARS AHEAD of schedule for cloud transformation

80+ APP TREATMENTS defined for cloud migration

OPTIMISED COSTS of cloud server resources

ABOUT THE AUTHORS

Lachlan is a seasoned technologist and a catalyst for accelerated change in large, highly regulated enterprises seeking to modernise their technology platforms and engineering culture. He partners closely with organisations across Government, Financial Services, and Commercial Enterprises in Australia and New Zealand, driving business value through innovative, creative solutions.

As CTO, Lachlan leads LAB³'s technology strategy, accelerators, and R&D. Under his leadership, LAB³ has developed a comprehensive catalogue of unique ready-made accelerators, designed to be deployed across any industry. These solutions build on Microsoft's offerings, enabling clients to accelerate cloud adoption quickly and securely.

LACHLAN WHITE
Chief Technology Officer, LAB³

Uniquely, Lachlan has been at the forefront of region launches with organisations through all three Australian Azure regions—Sydney, Melbourne, and Canberra. His deep experience has allowed him to guide organisations in maximising value during the release of new regions, helping them leverage these expansions to their strategic advantage. This experience has made him a sought-after expert for organisations looking to take full advantage of the latest cloud innovations in Australia and New Zealand.

Widely respected as an industry expert in cloud and digital transformation, Lachlan specialises in leveraging Microsoft Azure, Terraform, Cloud-Native Technologies, and, more recently, AI. Recognised as a leader in these fields, Lachlan has been a HashiCorp Ambassador for all five years since the program's inception, one of only three worldwide to achieve this. He was also previously an ambassador for the Cloud Native Computing Foundation (CNCF).

Lachlan has also featured as an international speaker, sharing his expertise at various conferences worldwide, where he continues to inspire organisations and technologists in their cloud and digital transformation journeys.

Stu is a seasoned cloud technology strategist and proven leader with extensive experience in Microsoft, Azure, and AWS cloud technologies.

Stu provides strategic advisory services for clients embarking on digital transformation initiatives, specialising in cloud / hybrid modernisation, adoption strategies & roadmapping, solution architecture, economic modelling and operational model improvements. His approach aims to enable new ways of working while fostering a culture of innovation and continuous improvement.

STU MCKENZIE
Principal Technologist, LAB³

Stu has collaborated with clients across commercial, government, education, utilities, and healthcare sectors throughout the Asia-Pacific region, particularly seeking to modernise legacy environments to cloud-native. He is passionate about solving real-world business challenges with technology, particularly leveraging AI to drive transformation and growth.

With over 15 years of industry experience, he has also led consultancy practices focused on cloud transformation, has authored numerous thought leadership articles, developed and led go-to-market (GTM) campaigns driven through LinkedIn, and contributed to the expansion of LAB3's service portfolio through development and execution of new service propositions.

LAB³

Your Cloud Transformation Partner in Aotearoa

info@lab3nz.co.nz

LAB3NZ.CO.NZ

Microsoft
Solutions Partner